明 細 書

不正監視プログラム、不正監視の方法及び不正監視システム

技術分野

[0001] 本発明は、コンピュータに不正な操作を実行させる不正データを監視するための不正監視プログラム、不正監視の方法及び不正監視システムに関するものである。

背景技術

[0002] コンピュータをインターネット等のネットワークに接続して使用する場合、外部からの不正なデータの侵入を防止するとともに、コンピュータの不正操作による内部からのデータ流出や漏洩を防止することが必要になる。不正なデータの侵入を防止するためには、企業内LANなどの内部ネットワークとインターネットの間にファイアウォールを設けて不正なデータを遮断することや、内部ネットワークや個々のコンピュータ端末にウィルスの侵入を防止するワクチンソフトを配置することが、広く行われている。ファイアウォールやワクチンソフトにおいては、キーワードや送信元のIPアドレスなどから不正なデータを判定するためのルールを予め定めておき、当該ルールを参照することにより不正なデータか否かを判定することが一般的である。

[0003] 一方、不正な操作によりデータが流出することを防止するための方法については、例えばネットワークに送出されるデータに対して、アクセス権や送信元、送信する文書の種類などについて予め定められたルールを参照して、不正の恐れがあると検知されると通信を切断する技術が開示されている(例えば、特許文献1参照)。

特許文献1:特開2002−232451号広報

発明の開示

発明が解決しようとする課題

[0004] ファイアウォールやワクチンソフト、前記特許文献1記載の発明は、いずれもネットワークにおける不正なデータの侵入や漏洩を防止するためのものである。しかしながら、コンピュータを用いた不正操作はネットワークを介するものに限られず、例えば権限のない第三者が外部ネットワークには接続されていないコンピュータを不正に操作して、コンピュータ内部の情報をプリンタに出力する、外部ディスクに書き出す、といっ

たネットワークを用いない方法による情報流出の危険性も存している。つまり、不正な操作を実行させるデータの監視は、ネットワークとの間だけでなく、プリンタやドライブと接続するドライバレベルにおいても行われることが好ましい。

[0005] また、先に説明した通り、現在の不正データの監視手法はキーワード、IPアドレスやMACアドレス等を登録したルールベースを主とするものであるが、かかる方法により登録できるルールの内容には限りがある。なるべく正確な判定を行うためにはルールの数を増加させることが好ましいが、ルールの数があまりに多くなっても、判定にかかる処理が重くなるという問題が生じる。従って、多様な切り口からのルールをなるべく簡潔に登録し、かつルールの参照を効率的に行うような仕組みがあると効果的である。

[0006] さらに、ルールベースによる不正判定は、従来とは全く異なる方法により、登録されたルールに該当しない不正な操作を実行されると、ルールベースのみではこれを感知し難いという問題も有している。これに対しては、従来と異なるユーザの操作行動のパターンを捉えて、不正の可能性を的確に判断することができると効果的である。

[0007] 本発明は、これらの課題に対応してなされたものであり、コンピュータに不正な操作を実行させる不正データの監視において、ネットワークのみでなく外部デバイスとの間で入出力されるデータの監視が可能であり、かつ不正判定のための多様なルール設定と効率的なルールの適用が可能な不正監視プログラム、不正監視の方法及び不正監視システムを提供することを目的とするものである。

課題を解決するための手段

[0008] 本願にかかる課題を解決する第1の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するステップと、前記入出力データからユーザを識別する識別情報を特定するステップと、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得するステップと、前記入出力データが不正データであると判定するルールを格納する判定ルール格

納部を参照して、前記入出力データが不正データであるかを判定するステップと、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作を停止させるステップと、を実行させ、前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データであるかを判定するステップにおいては、前記属性情報を取得するステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視プログラムである。

[0009] 第1の発明においては、ネットワークのみでなく、コンピュータの外部接続バスを通じて入出力されるデータを監視することにより、ネットワークを経由しない不正なプリントアウトやディスクへの書き込みなどの操作を指示するデータを監視して、不正な操作を中断させることができる。また、ユーザの属性情報に応じた判定項目を加えることにより、ルールの多様化を図ることができる。

[0010] 第1の発明において、コンピュータとは、ネットワークに接続され外部接続バスを備えていれば、ネットワークにおいてクライアントとして利用されるであってもよいし、サーバとして利用されるものであってもよい。ネットワークには、LAN、ダイヤルアップなどデータの送受信が可能な全てのネットワークが含まれる。外部デバイスは、プリンタやドライブなど、外部接続バスを通してコンピュータに接続可能な全ての周辺装置が含まれる。不正データとは、外部に流出が禁じられたファイルの送信指示、権限の無いユーザによる操作など、コンピュータの不正操作にかかるデータが該当する。ユーザの属性情報には、例えばユーザの年齢、性別、所属部署、役職などが用いられる。

[0011] また、第1の発明は、前記コンピュータに、前記ユーザ情報格納部を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定するステップと、前記利用権限を判定するステップにおいて利用権限が無いと判定された場合には、前記入出力データにより実行される操作を停止させるステップと、を実行させ、前記利用権限を判定するステップは、前記不正データを判定するステップより先行して実行され、前記利用権限を判定するステップにおいて利用権限が無いと判定された場合には、前記コンピュータに、前記属性情報を取得するステップ又は

前記不正データを判定するステップの少なくとも一つのステップを実行させないことを特徴とすることを特徴とすることもできる。

[0012] 第1の発明においては、ルールの一項目として用いるためにユーザの属性を予め登録するので、操作を行ったユーザがコンピュータの利用権限を有するものか否かを容易に確認することができる。ユーザの利用権限の有無をルールの判定前に行うこととすれば、最初の段階でそもそも権限を有しないユーザの操作である場合には、ルールを適用する前に操作の停止処理を行うことにより、ルールを適用する処理を効率化することができる。

[0013] さらに、第1の発明は、前記コンピュータに、前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納部を参照して、前記データ取得ステップにおいて取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異であるかを判定するステップを実行させ、前記入出力データにより実行される操作を停止させるステップにおいては、前記特異であるかを判定するステップにおいて特異であると判定された場合にも、前記入出力データにより実行される操作を停止させることを特徴とすることもできる。

[0014] このようにユーザ毎のログデータの収集によりユーザ毎の操作の特性を把握したプロファイルを作成し、かかるプロファイルを参照してユーザが特異な操作を行ったか否かを判定することにより、ルールでは判断することのできない第三者による権限のあるユーザへのなりすまし、権限の範囲内ではあるが通常は実行しない不正の可能性のある操作などを判定することが可能になる。

[0015] さらに、第1の発明は、前記入出力データを取得するステップにおいて、ネットワークから前記入出力データを取得した場合には、前記入出力データにより実行される操作を停止させるステップにおいては、セッションの切断処理を実行させることを特徴とすることもできる。

[0016] さらに、第1の発明は、前記入出力データを取得するステップにおいて、外部接続バスから前記入出力データを取得した場合には、前記入出力データにより実行される操作を停止させるステップにおいては、ドライバの実行する処理を停止させることを特徴としてもよい。

[0017] 第1の発明においては、コンピュータが実行中の処理が不正操作であると判定された場合には、即時に実行を停止させるための処理がなされる。実行中の処理がネットワークを通じたデータの送受信である場合には、実行中のセッションの切断処理を行うことにより、データの外部送信による情報漏洩等を防止することができる。実行中の処理が外部接続バスを通じた外部デバイスへの操作である場合には、ドライバの実行する処理を停止させることにより、データの出力による情報漏洩等を防止することができる。

[0018] 本願にかかる課題を解決する第2の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するステップと、前記入出力データからユーザを識別する識別情報を特定するステップと、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得するステップと、前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定するステップと、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知するステップと、を実行させ、前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データを判定するステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視プログラムである。

[0019] この発明においては、第1の発明は不正データと判定すると当該データにより実行される処理を停止させるのに対し、当該データにかかる処理を実行させた操作者であるユーザ、又はコンピュータや端末の管理者に対して警告を通知することにより、不正データに対処することを特徴している。

[0020] 第1の発明及び第2の発明は、上記の不正監視プログラムを実行することによる不

正監視の方法として特定することもできる。また、上記の不正監視プログラムを用いた不正監視システムとして構成することもできる。

[0021] つまり、第1の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段と、前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作を停止させる停止手段と、を備えていて、前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データ判定手段においては、前記属性情報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視システムとして構成することもできる。

[0022] また、第1の発明は、前記ユーザ情報格納部を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定する利用権限判定手段を備えていて、前記停止手段は、前記利用権限判定手段において利用権限が無いと判定された場合にも、前記入出力データにより実行される操作を停止させ、前記利用権限判定手段は、前記不正データ判定手段より先行して起動され、前記利用権限判定手段によって利用権限が無いと判定された場合には、前記属性情報取得手段又は前記不正データ判定手段の少なくとも一つの手段が起動されないことを特徴とすることもできる。

[0023] さらに、第1の発明は、前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納手段と、前記プロファイル格納手段を参照して

、前記データ取得手段において取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異であるかを判定する特異操作判定手段と、を備えていて、前記停止手段は、前記特異操作判定手段において特異と判定された場合にも、前記入出力データにより実行される操作を停止させることを特徴とすることもできる。

[0024] さらに、第1の発明は、前記データ取得手段が、ネットワークから前記入出力データを取得した場合には、前記停止手段はセッションの切断処理を実行することを特徴とすることもできる。

[0025] さらに、第1の発明は、前記データ取得手段が、外部接続バスから前記入出力データを取得した場合には、前記停止手段はドライバの実行する処理を停止させることを特徴とすることもできる。

[0026] 第2の発明は、コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段と、前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知する通知手段と、を備えていて、前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、前記不正データ判定手段においては、前記属性情報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定することを特徴とする不正監視システムとして構成することもできる。

発明の効果

[0027] 本発明により、コンピュータに不正な操作を実行させる不正データの監視において、ネットワークのみでなく外部デバイスとの間で入出力されるデータの監視が可能となり、なりすましや権限の無い者による不正なデータ出力による情報漏洩等を防止することができる。

[0028] また、ルールの一項目に予め登録されたユーザの属性情報を用いることにより、不正判定のための多様なルール設定を行うことが可能になる。さらに、属性情報を用いてコンピュータの操作権限の有無をルールの適用に先立って判定することにより、不正判定にかかる処理を効率化することができる。さらに、ユーザ毎の操作履歴をプロファイルとして記録することにより、ルールでは判断できない特異な操作パターンを認識し、権限のあるユーザへのなりすまし、権限の範囲内ではあるが通常は実行しない不正の可能性のある操作などを判定することも可能になる。

発明を実施するための最良の形態

[0029] 本発明を実施するための最良の形態について、図面を用いて以下に詳細に説明する。尚、以下の説明は本発明の実施形態の一例であって、本発明はかかる実施形態に限定されるものではない。

[0030] 図1、図2は、本発明にかかる不正監視システムを、それぞれネットワークの監視、外部デバイスとの接続の監視に用いる例を示す図である。図3は、本発明にかかる不正監視システムの設置位置を示す図である。図4、図5は、本発明にかかる不正監視システムの第一の構成を示すブロック図である。図6は、本発明にかかる不正監視システムのユーザデータ格納部の一例を示す図である。図7は、本発明にかかる不正監視システムの不正ルール格納部の一例を示す図である。図8は、本発明にかかる不正監視プログラムのフローを示すフローチャートである。

[0031] 本発明にかかる不正監視システムは、ネットワークに流れる各種のデータを監視するだけでなく、プリンタなどの出力装置や外部ディスクドライブなどの外部記憶装置をはじめとする外部デバイスと接続するための外部接続バスの監視も行うことができることを特徴としている。図3に示したとおり、本発明にかかる不正監視システムは、企業内LANなどの内部ネットワークとインターネットのゲートウェイに設けられてネットワークを監視してもよいし、メールサーバに設けられてネットワークを通じたメールの送受

信を監視してもよい。また、内部ネットワークにおけるセグメントの監視に用いてもよいし、個々のユーザ端末とネットワークとの監視、若しくは外部デバイスとの接続の監視に用いてもよい。

[0032] 図1は、ネットワークの監視に用いる場合の一例であり、本発明にかかる不正監視システムは、不正監視サーバ10、ユーザデータ格納部12及び不正ルール格納部13により構成されている。不正監視サーバ10は、内部ネットワークとインターネットのゲートウェイに設けられて内部ネットワーク全体からの不正なデータの漏洩等を監視するものであってもよいし、内部ネットワークに設けられてセグメント内における不正なデータの漏洩等の監視に用いられるものであってもよい。

[0033] 不正監視サーバ10では、ネットワークを流れる全ての入出力データを取得し、ユーザデータ格納部12からデータの入出力を行うユーザの属性にかかる情報を取得する。不正ルール格納部13には、一般的な不正データの判定ルールに加えて、ユーザの属性に応じて不正と判定されるルールが格納されており、不正監視サーバ10は不正ルール格納部13を参照して当該入出力データについて一般的な判定ルールを参照するとともに、ユーザデータ格納部12から取得した属性に対応するルールを参照して、当該入出力データが不正か否かの判定を行う。不正と判定された入出力データに対しては、入出力が行われようとしたセッションの遮断処理を実行する。

[0034] 図2は、外部接続バスの監視に用いる場合の一例であり、本発明にかかる不正監視システムは、処理装置210のHDD214に格納された不正監視プログラム11、ユーザデータ格納部12及び不正ルール格納部13により構成されていて、これらのプログラムや格納されたデータは、監視の実行時にHDD214から読み出されて、処理装置210において演算処理される。処理装置210においては、HDD214に格納された不正監視プログラム11による監視を実行するために、ROM213に記憶された入力制御や出力制御などのハードウェア制御のための基本的な各種プログラムを起動して、RAM212を不正監視プログラム11のワークエリアとして機能させながら、CPU211が演算処理を行う。不正監視プログラム11の演算処理においては、HDD214のユーザデータ格納部12及び不正ルール格納部13より必要なデータが読み出されて用いられる。尚、処理装置においてプログラムを格納するHDD214については、フラ

ッシュメモリなどプログラムを格納することができるその他の記憶媒体を用いるものであってもよい。

[0035] 不正監視プログラム11は、処理装置210においてドライバプログラム22が読み出されて外部接続バス23にプリントアウトや外部ディスク等への書き出しの指示データが送信されると、外部接続バス23を流れる指示データを取得し、ユーザデータ格納部12から当該指示データにかかる操作を行ったユーザの属性にかかる情報を取得する。不正ルール格納部13には、一般的な不正データの判定ルールに加えて、ユーザの属性に応じて不正と判定されるルールが格納されており、不正監視プログラム11は当該指示データが不正ルール格納部13に格納された一般的な判定ルールに該当するかを判定するとともに、ユーザデータ格納部12から取得した属性に対応するルールに該当するかを判定する処理を実行する。不正と判定された指示データに対しては、ドライバプログラム22により実行された処理を停止させるための処理、例えばプリントアウトの停止や外部接続バス23に直接接続されたコンピュータとの通信の停止などの処理を実行する。

[0036] 図1の不正監視サーバ10、及び図2の不正監視プログラム11における不正判定の方法について、図4及び図5を用いてさらに詳しく説明する。図4は、不正の判定ルールにユーザの属性に応じたルールを加えた判定方式を、図5はルールベースのみでなく、ユーザ毎のプロファイルから操作パターンを判定して特異な操作を不正と判定する方式を実行するための構成を示したものである。

[0037] 図4における不正の判定は、データ取得部14による判定の対象となるデータの取得、不正操作判定部15によるルールベースの不正操作の判定、中断処理実行部16による対象となる処理の中止、の順により行われる。尚、これらの各部は物理的に分離されているものではなく、各々を実行する不正監視プログラム11の一部のプログラムとしてHDD214に格納されており、順次読み出されてRAM212をワークエリアとして機能させながら、CPU211により演算処理が実行されるものであってもよい。

[0038] データ取得部14は、ネットワーク又は外部接続バスを流れるデータを取得する。取得するデータには、当該データにかかる操作を実行したユーザの識別データが含まれている。識別データは、ユーザがコンピュータにログインした際のログインID等によ

り特定される。

[0039] 不正操作判定部15においては、ユーザデータ格納部12から、データ取得部14で取得したユーザの識別データに対応するユーザの属性情報を取得する。図6は、ユーザデータ格納部12に格納されたユーザの属性情報の一例であり、ユーザ毎に設けられたレコードには、ユーザIDと、部署や職種などの属性情報が格納されている。

[0040] 次に、不正操作判定部15は、不正ルール格納部13を参照して、データ取得部14で取得したデータが不正と判定すべきルールに該当するか否かを判定する。不正ルール格納部13には、ユーザの属性に関わらず一般的に不正と判定すべきルールと、ユーザの属性に応じて許可されない事項を定めた属性毎のルールが格納されている。前者については、例えばキーワード、URL、IPアドレス、MACアドレスなどを基準に、不正の判定に一般的に用いられているルールが該当する。後者については、例えば部署や役職に応じて特定の操作について定められた操作権限などが該当する。

[0041] 図7は不正ルール格納部13に格納されたユーザの属性に応じて定められた判定ルールの一例であるが、ルール単位で設けられたレコードには、対象となる属性と適用されるルールが格納されており、この例では正社員以上にのみメールの送信権限を付与している。例えば、図6の例に示したインターンの看護士がメールを送信しようとすると、送信権限がないと判断されて、メールの送信処理が停止されることになる。

[0042] このように不正操作判定部15において取得したデータにかかる操作が不正な操作であると判定されると、中断処理実行部16において当該操作により実行される処理を停止させるための処理が実行される。つまり、ネットワークを通じた入出力データに対しては、入出力が行われようとしたセッションの遮断処理が実行され、外部接続バスを通じた実行処理データに対しては、プリントアウトの停止や外部ディスクへの書き込みの停止などの処理が実行される。

[0043] 尚、不正操作判定部15においては、ユーザデータ格納部12からユーザの属性情報を取得する際に、ユーザIDに該当するデータが存在しない場合、又はユーザIDが当該ユーザの退職等により無効とされている場合には、無権限者によるアクセスとして、不正ルール格納部13による判定を行わずに不正と判定して、中断処理実行部

16による中断を実行することとしてもよい。このようにルールベースの判定の前に無権限者によるアクセスを判定すると、システムの処理負担を軽減し、速やかな判定と中断処理を実行することが可能になる。

[0044] 図5における不正の判定は、データ取得部14による判定の対象となるデータの取得、不正操作判定部15によるルールベースの不正操作の判定、特異操作判定部18によるルールベースによらないユーザ毎の操作パターンからの不正操作の判定、中断処理実行部16による対象となる処理の中止、がそれぞれ実行される。尚、これらの各部については物理的に分離されたものではなく、各々を実行する不正監視プログラム11の一部のプログラムとしてHDD214に格納されており、順次読み出されてRAM212をワークエリアとして機能させながら、CPU211により演算処理が実行されるものであってもよいのは、図4の場合と同様である。

[0045] 図5においても、データ取得部14による判定の対象となるデータの取得と、不正操作判定部15によるルールベースの不正操作の判定、中断処理実行部16による対象となる処理の中止についての処理は、図4の場合と同様である。この構成においては、プロファイル作成部19においてユーザ毎のプロファイルを作成し、特異操作判定部18ではユーザ毎の操作パターンから不正操作を判定する点に特徴を備えている。

[0046] データ取得部14において取得されたデータは、ルールベースによる判定を行う不正操作判定部15とともに、ユーザ毎の操作パターンによる判定を行う特異操作判定部18により判定が実行される。ユーザプロファイル17には各々のユーザの過去の操作パターンが登録されており、特異操作判定部18では取得したデータにかかる操作とユーザプロファイル17に登録された当該ユーザの操作パターンを対比して、特異な操作であると判定する場合には、中断処理実行部16による中断を実行する。例えば、通常は操作を行わない時間帯に操作を行った場合、通常は実行しないタイプの操作を大量に実行した場合などは、当該ユーザによる不正行為や他人のユーザIDを用いたなりすましである可能性があるとして、処理が中断される。

[0047] 尚、ユーザプロファイル17へ登録される操作パターンは、特異操作判定部18において判定に用いたデータと、ユーザデータ格納部12のユーザの属性情報から作成す

ることができる。データ取得部14において取得したデータのログを用いることとしてもよい。プロファイルの更新は、新たなデータを取得する毎にオンライン処理として実行してもよいし、定期的なバッチ処理により行ってもよい。

[0048] 特異操作判定部18には、ユーザプロファイル17に比して特異な操作パターンを判定するための、知識エンジンが設けられている。知識エンジンは通常の操作と特異な操作を判別する人工知能の機能を備えているが、人工知能の構造はベイジアン・ネットワークによるものであってもよいし、ニューラル・ネットワークによるものであってもよい。

[0049] 尚、これまで説明した実施形態においては、不正操作と判定されるとセッションの遮断処理が実行され、外部接続バスを通じた実行処理データに対しては、プリントアウトの停止や外部ディスクへの書き込みの停止などの処理が実行されることとして更正しているが、不正操作と判定された場合には、当該操作を実行したユーザや、コンピュータやネットワークの管理者に対して警告を通知するよう構成してもよい。

[0050] 図8のフローチャートを用いて、本発明にかかる不正監視プログラムの基本的なフローについて説明する。まず、ネットワーク又は外部接続バスを流れる入出力データと、当該入出力データにかかる操作を実行した操作者のIDを取得する(S01)。取得したIDについて、ユーザの属性情報を格納するユーザデータベースを参照し(S02)、ユーザデータベースに当該IDが存在しない場合には(S03)、操作権限の無い者による操作と判断して、当該入出力データにかかる操作の中止処理を実行する(S08)。

[0051] ユーザデータベースに当該IDが存在する場合には(S03)、当該IDにかかる属性情報をユーザデータベースから取得する(S04)。続いてルールデータベースを参照して(S05)、まず取得した属性が属性毎に定められたルールに該当しないかを判定する(S06)。該当する場合には、当該操作にかかる操作権限の無い者による操作と判断して、当該入出力データにかかる操作の中止処理を実行する(S08)。該当しない場合には、続いて取得した入出力データが一般的なルールに該当しないかを判定する(S07)。該当する場合には、当該操作は不正な操作であると判断して、当該入出力データにかかる操作の中止処理を実行する(S08)。該当しない場合には、正

常な操作であるとして、そのまま当該入出力データにかかる操作が実行される。

図面の簡単な説明

[0052] [図1]本発明にかかる不正監視システムを、ネットワークの監視に用いる例を示す図である。

[図2]本発明にかかる不正監視システムを、外部デバイスとの接続の監視に用いる例を示す図である。

[図3]本発明にかかる不正監視システムの設置位置を示す図である。

[図4]本発明にかかる不正監視システムの第一の構成を示すブロック図である。

[図5]本発明にかかる不正監視システムの第二の構成を示すブロック図である。

[図6]本発明にかかる不正監視システムのユーザデータ格納部の一例を示す図である。

[図7]本発明にかかる不正監視システムの不正ルール格納部の一例を示す図である。

[図8]本発明にかかる不正監視プログラムのフローを示すフローチャートである。

符号の説明

[0053] 10 不正監視サーバ
11 不正監視プログラム
12 ユーザデータ格納部
13 不正ルール格納部
14 データ取得部
15 不正操作判定部
16 中断処理実行部
17 ユーザプロファイル
18 特異操作判定部
19 プロファイル作成部
20 ユーザ端末
210 処理装置
211 CPU

212 RAM

213 ROM

214 HDD

22 ドライバプログラム

23 外部接続バス

24 出力装置

25 外部記憶装置

31 ユーザ端末

32 ユーザ端末

33 ユーザ端末

41 外部端末

42 外部端末

43 外部端末

請求の範囲

[1] コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、

前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するステップと、

前記入出力データからユーザを識別する識別情報を特定するステップと、

前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得するステップと、

前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定するステップと、

前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作を停止させるステップと、を実行させ、

前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、

前記不正データであるかを判定するステップにおいては、前記属性情報を取得するステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること

を特徴とする不正監視プログラム。

[2] 前記コンピュータに、

前記ユーザ情報格納部を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定するステップと、

前記利用権限を判定するステップにおいて利用権限が無いと判定された場合には、前記入出力データにより実行される操作を停止させるステップと、を実行させ、

前記利用権限を判定するステップは、前記不正データを判定するステップより先行して実行され、

前記利用権限を判定するステップにおいて利用権限が無いと判定された場合には、前記コンピュータに、前記属性情報を取得するステップ又は前記不正データを判定

するステップの少なくとも一つのステップを実行させないこと
を特徴とする請求項1記載の不正監視プログラム。

[3] 前記コンピュータに、
前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプロファイル格納部を参照して、前記データ取得ステップにおいて取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異であるかを判定するステップを実行させ、
前記入出力データにより実行される操作を停止させるステップにおいては、前記特異であるかを判定するステップにおいて特異であると判定された場合にも、前記入出力データにより実行される操作を停止させること
を特徴とする請求項1記載の不正監視プログラム。

[4] 前記入出力データを取得するステップにおいて、ネットワークから前記入出力データを取得した場合には、前記入出力データにより実行される操作を停止させるステップにおいては、セッションの切断処理を実行させること
を特徴とする請求項1乃至3いずれかに記載の不正監視プログラム。

[5] 前記入出力データを取得するステップにおいて、外部接続バスから前記入出力データを取得した場合には、前記入出力データにより実行される操作を停止させるステップにおいては、ドライバの実行する処理を停止させること
を特徴とする請求項1乃至3いずれかに記載の不正監視プログラム。

[6] コンピュータに不正な操作を実行させる不正データを監視するためのプログラムであって、前記コンピュータに、
前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するステップと、
前記入出力データからユーザを識別する識別情報を特定するステップと、
前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得するステップと、
前記入出力データが不正データであると判定するルールを格納する判定ルール格

納部を参照して、前記入出力データが不正データであるかを判定するステップと、
前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知するステップと、を実行させ、
前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データを判定するステップにおいては、前記属性情報取得ステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視プログラム。

[7] コンピュータに不正な操作を実行させる不正データを監視するための方法であって、
前記コンピュータが、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するステップと、
前記コンピュータが、前記入出力データからユーザを識別する識別情報を特定するステップと、
前記コンピュータが、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得するステップと、
前記コンピュータが、前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定するステップと、
前記コンピュータが、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作を停止させるステップと、を有していて、
前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データを判定するステップにおいては、前記属性情報を取得するステップ

において取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視の方法。

[8] コンピュータに不正な操作を実行させる不正データを監視するための方法であって、
前記コンピュータが、前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するステップと、
前記コンピュータが、前記入出力データからユーザを識別する識別情報を特定するステップと、
前記コンピュータが、前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納部から、前記識別情報に対応する属性情報の少なくとも一部を取得するステップと、
前記コンピュータが、前記入出力データが不正データであると判定するルールを格納する判定ルール格納部を参照して、前記入出力データが不正データであるかを判定するステップと、
前記コンピュータが、前記不正データ判定ステップにおいて不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知するステップと、を有していて、
前記判定ルール格納部には、ユーザの属性に対応する判定ルールが記憶されていて、
前記不正データを判定するステップにおいては、前記属性情報を取得するステップにおいて取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること
を特徴とする不正監視の方法。

[9] コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、
前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段

と、

前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、

前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、

前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、

前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、

前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、

前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作を停止させる停止手段と、を備えていて、

前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、

前記不正データ判定手段においては、前記属性情報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること

を特徴とする不正監視システム。

[10] 前記ユーザ情報格納部を参照して、前記識別情報に対応するユーザが前記コンピュータの利用権限を有しているかを判定する利用権限判定手段を備えていて、

前記停止手段は、前記利用権限判定手段において利用権限が無いと判定された場合にも、前記入出力データにより実行される操作を停止させ、

前記利用権限判定手段は、前記不正データ判定手段より先行して起動され、

前記利用権限判定手段によって利用権限が無いと判定された場合には、前記属性情報取得手段又は前記不正データ判定手段の少なくとも一つの手段が起動されないこと

を特徴とする請求項9記載の不正監視システム。

[11] 前記入出力データにかかるログデータを、ユーザ毎のプロファイルとして格納するプ

ロファイル格納手段と、

前記プロファイル格納手段を参照して、前記データ取得手段において取得された入出力データが前記ユーザの日常的な操作の傾向に比して特異であるかを判定する特異操作判定手段と、を備えていて、

前記停止手段は、前記特異操作判定手段において特異と判定された場合にも、前記入出力データにより実行される操作を停止させること

を特徴とする請求項9記載の不正監視システム。

[12] 前記データ取得手段が、ネットワークから前記入出力データを取得した場合には、前記停止手段はセッションの切断処理を実行すること

を特徴とする請求項9乃至11いずれかに記載の不正監視システム。

[13] 前記データ取得手段が、外部接続バスから前記入出力データを取得した場合には、前記停止手段はドライバの実行する処理を停止させること

を特徴とする請求項9乃至11いずれかに記載の不正監視システム。

[14] コンピュータに不正な操作を実行させる不正データを監視するためのシステムであって、

前記コンピュータに接続されたネットワーク又は前記コンピュータと外部デバイスを接続する外部接続バスを通じて入出力される入出力データを取得するデータ取得手段と、

前記入出力データからユーザを識別する識別情報を特定する識別情報特定手段と、

前記コンピュータの利用権限を有するユーザについて各々のユーザの属性情報を格納するユーザ情報格納手段と、

前記ユーザ情報格納手段から、前記識別情報に対応する属性情報の少なくとも一部を取得する属性情報取得手段と、

前記入出力データが不正データであると判定するルールを格納する判定ルール格納手段と、

前記判定ルール格納手段を参照して、前記入出力データが不正データであるかを判定する不正データ判定手段と、

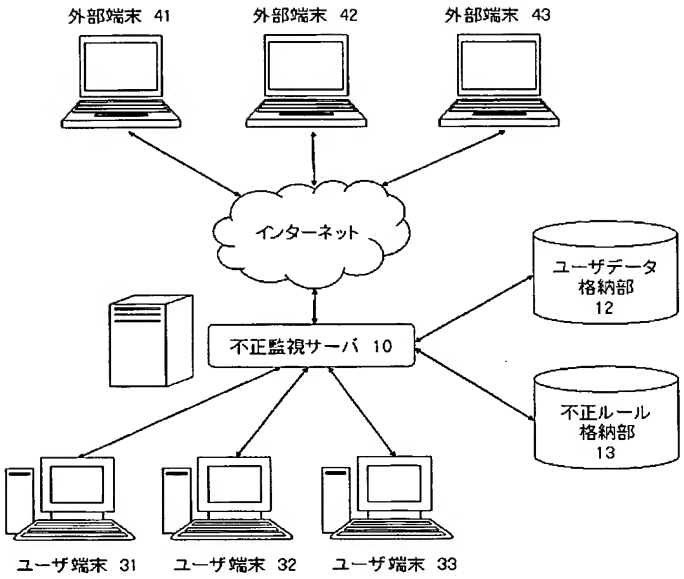
前記不正データ判定手段において不正データであると判定された場合には、前記入出力データにより実行される操作が不正な操作であることを前記ユーザ又は管理者の操作する端末装置に通知する通知手段と、を備えていて、

前記判定ルール格納手段には、ユーザの属性に対応する判定ルールが記憶されていて、

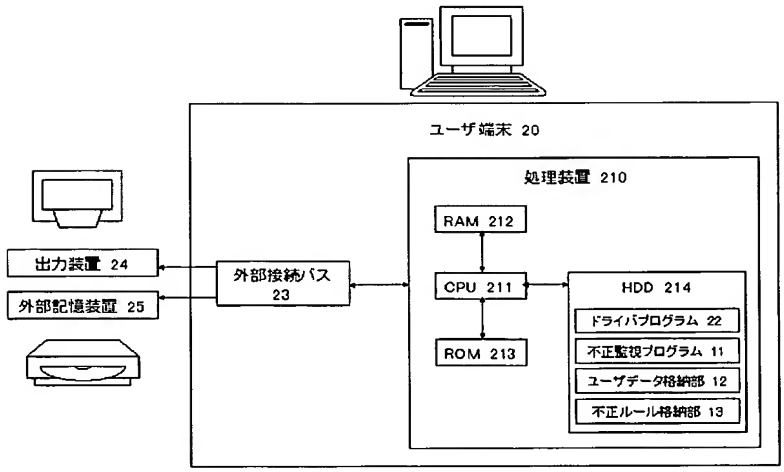
前記不正データ判定手段においては、前記属性情報取得手段が取得した属性情報に対応する前記判定ルールを参照して、不正データであるかを判定すること

を特徴とする不正監視システム。

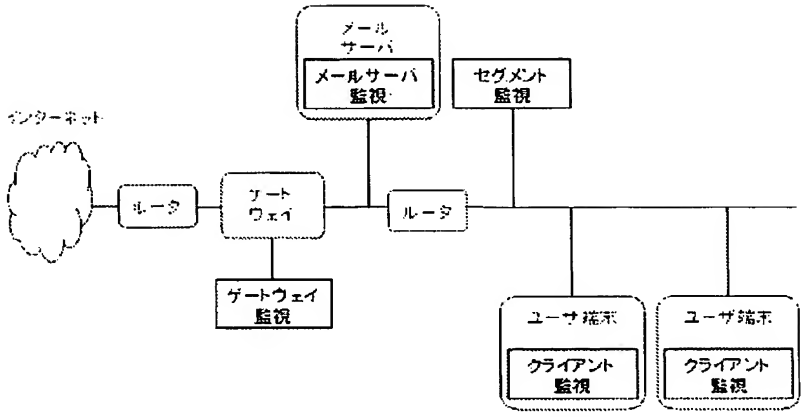
[図1]


外部端末 41
外部端末 42
外部端末 43
インターネット
ユーザデータ格納部 12
不正監視サーバ 10
不正ルール格納部 13
ユーザ端末 31
ユーザ端末 32
ユーザ端末 33

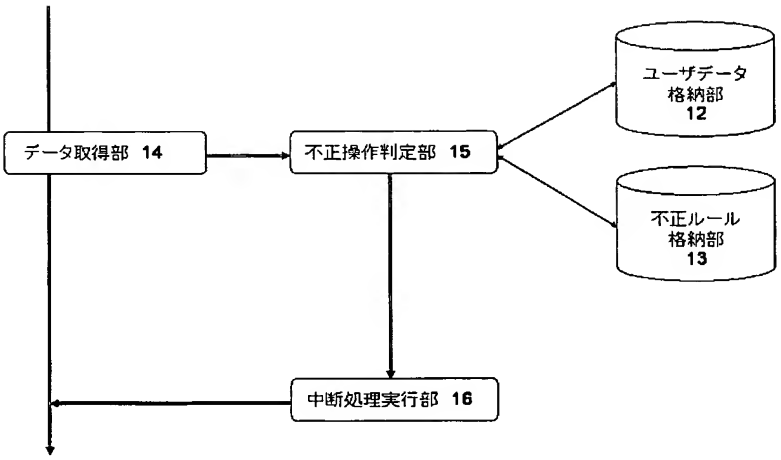
[図2]


ユーザ端末 20
処理装置 210
RAM 212
CPU 211
ROM 213
HDD 214
ドライバプログラム 22
不正監視プログラム 11
ユーザデータ格納部 12
不正ルール格納部 13
出力装置 24
外部記憶装置 25
外部接続バス 23

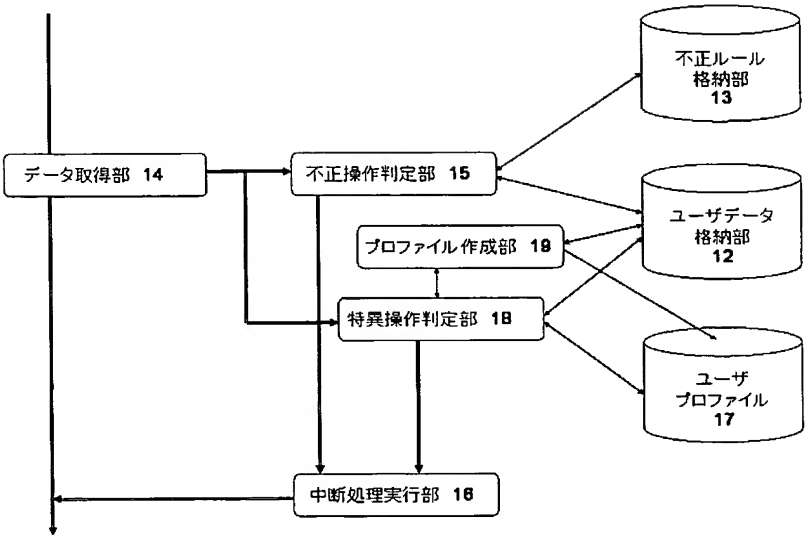
[図3]


メール
サーバ
メールサーバ
監視
セグメント
監視
インターネット
ルータ
ゲート
ウェイ
ルータ
ゲートウェイ
監視
ユーザ端末
クライアント
監視
ユーザ端末
クライアント
監視

[図4]


ユーザデータ
格納部
12
データ取得部 14
不正操作判定部 15
不正ルール
格納部
13
中断処理実行部 16

[図5]



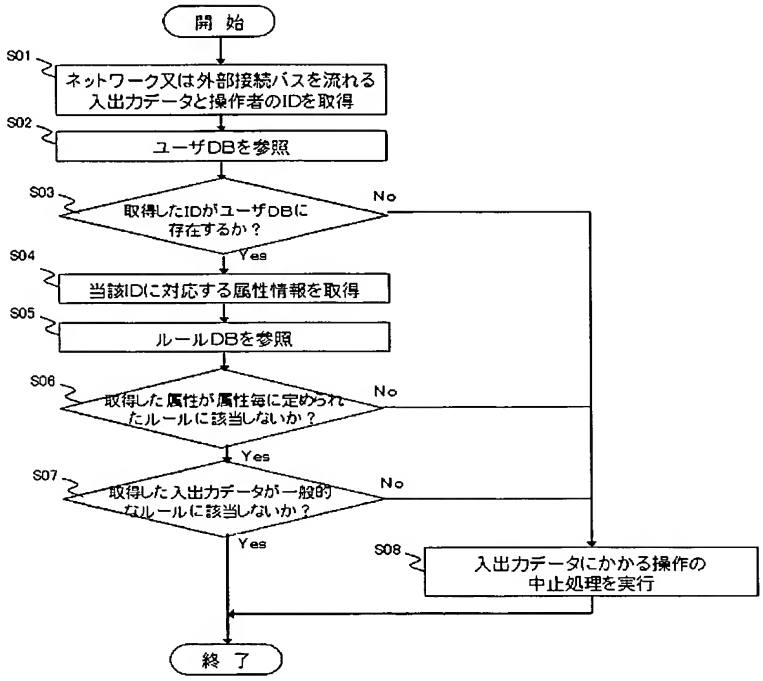
[図6]

ユーザID	0001
ユーザネーム	○○ ××
部署	外科
部門	第2
職種	看護士
役職	一般
ステータス	インターン

[図7]

ルールコード	a1111
部署	外科
部門	第2
動作	メール送信
ルール	正社員以上

[図8]


開 始
S01
ネットワーク又は外部接続バスを流れる入出力データと操作者のIDを取得
S02
ユーザDBを参照
S03
取得したIDがユーザDBに存在するか？
No
Yes
S04
当該IDに対応する属性情報を取得
S05
ルールDBを参照
S06
取得した属性が属性毎に定められたルールに該当しないか？
No
Yes
S07
取得した入出力データが一般的なルールに該当しないか？
No
Yes
S08
入出力データにかかる操作の中止処理を実行
終 了

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009860

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F13/00, G06F15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F13/00, G06F15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 5-120194 A (NEC Engineering Kabushiki Kaisha), 18 May, 1993 (18.05.93), All pages; all drawings (Family: none)	1-14
Y	JP 2003-296193 A (Seiko Instruments Inc.), 17 October, 2003 (17.10.03), All pages; all drawings; particularly, Par. No. [0031] (Family: none)	1-14
Y	JP 11-25045 A (NEC Corp.), 29 January, 1999 (29.01.99), All pages; all drawings; particularly, Fig. 2 (Family: none)	1-14

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 September, 2004 (09.09.04)	28 September, 2004 (28.09.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/009860

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-288087 A (Humming Heads Inc.), 04 October, 2002 (04.10.02), All pages; all drawings (Family: none)	1-14
A	JP 2003-44297 A (Humming Heads Inc.), 14 February, 2003 (14.02.03), All pages; all drawings & US 2002/0099837 A1	1-14
A	JP 2003-233521 A (Hitachi, Ltd.), 22 August, 2003 (22.08.03), All pages; all drawings (Family: none)	1-14
A	JP 2002-232451 A (Reiya Sebun Kabushiki Kaisha), 16 August, 2002 (16.08.02), All pages; all drawings (Family: none)	1-14

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／００９８６０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl.[7]　G06F12/14, G06F13/00, G06F15/00

Ｂ．　調査を行った分野
調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl.[7]　G06F12/14, G06F13/00, G06F15/00

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2004年
日本国実用新案登録公報　1996－2004年
日本国登録実用新案公報　1994－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 5-120194 A（日本電気エンジニアリング株式会社） 1993.05.18，全頁，全図（ファミリーなし）	1-14
Y	JP 2003-296193 A（セイコーインスツルメンツ株式会社） 2003.10.17，全頁，全図，特に【００３１】段落 （ファミリーなし）	1-14
Y	JP 11-25045 A（日本電気株式会社） 1999.01.29，全頁，全図，特に【図２】（ファミリーなし）	1-14

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
09.09.2004	28.9.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	5Ｎ	３０４４
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	髙橋　克		
	電話番号　０３－３５８１－１１０１　内線　３５８５		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

国際調査報告

国際出願番号　PCT／JP2004／009860

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 2002-288087 A (ハミングヘッズ株式会社) 2002.10.04, 全頁, 全図 (ファミリーなし)	1-14
A	JP 2003-44297 A (ハミングヘッズ株式会社) 2003.02.14, 全頁, 全図 & US 2002/0099837 A1	1-14
A	JP 2003-233521 A (株式会社日立製作所) 2003.08.22, 全頁, 全図 (ファミリーなし)	1-14
A	JP 2002-232451 A (レイヤーセブン株式会社) 2002.08.16, 全頁, 全図 (ファミリーなし)	1-14